IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND the claims in accordance with the following:

1. (CURRENTLY AMENDED) A central processing unit executing a program, comprising:

an encrypting unit encrypting a block~~,~~ and decrypting an encrypted block~~,~~; and

a tamper resistant buffer that a user cannot reference or falsify,

wherein:

a first private key is concealed in secrecy~~; and~~,

said encrypting unit obtains from a first license a code decryption key for decrypting an encrypted block which configures a first program by decrypting with the first private key the first license of the first program, which is encrypted with a public key pairing with the first private key~~.~~,

the code decryption key is recorded to said tamper resistant buffer~~;~~,

the first license includes an access condition used when an execution process of the first program accesses a memory region, and

wherein said central processing unit further includes:

a Translation Lookaside Buffer (TLB) recording an address of the memory region, at which the encrypted block which configures the first program is recorded, and the access condition to the memory region,

a memory managing unit,

a cache, and

a processor core,

wherein said TLB and said tamper resistant buffer are linked,

wherein said memory managing unit obtains the access condition to the memory region from said TLB based on an address or a memory region, at which an encrypted block is recorded, and further obtains the code decryption key corresponding to the memory region from said tamper resistant buffer,

wherein said processor core determines whether an access to the memory region is permitted to be made from the execution process based on the access condition obtained by

said memory managing unit, and the access to the memory region is made from the execution process if said processor core determines that the access to the memory region is permitted to be made and,

wherein said encrypting unit writes to said cache a code obtained by decrypting the encrypted block within the memory region with the code decryption key obtained by said memory managing unit.

2. (WITHDRAWN- CURRENTLY AMENDED) The central processing unit according to claim 1, ~~further comprising a cache, and~~ wherein said encrypting unit decrypts the encrypted block in units of cache when the encrypted block which configures the first program is output from a memory region to said cache.

3. (CANCELLED)

4. (CANCELLED)

5. (CURRENTLY AMENDED) The central processing unit according to ~~claim 4~~claim 1, wherein the code decryption key and the encryption key used to encrypt the encrypted block are a same key.

6. (CURRENTLY AMENDED) The central processing unit according to ~~claim 4~~claim 1, wherein when a memory region accessed from the execution process of the first program switches from a first memory region to a second memory region, said memory managing unit further determines whether or not a code decryption key corresponding to the first memory region, which is obtained from said tamper resistant buffer, and a code decryption key corresponding to the second memory region match, and an access is made to the second memory region from the execution process if said memory managing unit determines that the code decryption keys match, or the access to the second memory region is not made from the execution process if said memory managing unit determines that the code decryption keys mismatch.

7. (WITHDRAWN) The central processing unit according to claim 2, wherein the first license is buried in the first program.

8. (CURRENTLY AMENDED) The central processing unit according to ~~claim 4~~claim 1, wherein:

a different data encryption key is recorded to said tamper resistant buffer for each code decryption key;

said encrypting unit records data within said cache to the memory region that is corresponded to the data decryption key by said TLB after encrypting the data with the data decryption key when recording the data to the memory region, and writes encrypted data within the memory region to said cache after decrypting the read data with the data encryption key when reading the encrypted data within the memory region.

9. (ORIGINAL) The central processing unit according to claim 8, wherein when data obtained by executing a first code is used by a second code, said processor core sets said TLB so as to provide the second code with an access right to a memory region to which the data is recorded, and also sets said TLB and said tamper resistant buffer so that the second code uses a data encryption key for encrypting the data when reading the data from the memory region.

10. (CURRENTLY AMENDED) The central processing unit according to ~~claim 4~~claim 1, further comprising:

a register; and

a register access control table for performing access control for said register,

wherein said processor core controls sealing and release of said register with a sealing flag within said register access control table.

11. (CURRENTLY AMENDED) The central processing unit according to ~~claim 4~~claim 1, wherein when contents of said TLB is recorded to a page table within an external storage device, said encrypting unit affixes a signature to the contents to be recorded, and verifies whether or not the signature is legal when contents of the page table is captured into said TLB.

12. (CURRENTLY AMENDED) The central processing unit according to ~~claim 3~~claim 1, wherein when contents of said tamper resistant buffer is recorded to an encryption key table within an external storage device, said encrypting unit encrypts the contents to be recorded.

13. (WITHDRAWN) The central processing unit according to claim 2, which is connected to a different central processing unit, wherein:

a session key is obtained by making mutual authentication with the different central processing unit; and

said encrypting unit encrypts contents of said cache with the session key, and synchronously transfers the contents to the different central processing unit.

14. (WITHDRAWN) The central processing unit according to claim 2, wherein said encrypting unit obtains a private key encryption key used when a second private key is encrypted by decrypting a second license added to a second program with a public key before the first program is executed, and decrypts the second private key with the obtained private key encryption key.

15. (WITHDRAWN) The central processing unit according to claim 14, wherein:

an access condition indicating that only a read can be made from an execution process of the first program is added to the second license; and

the second private key can be read only from the execution process of the first program.

16. (WITHDRAWN) The central processing unit according to claim 14, wherein the second private key is encrypted with a data encryption key and recorded to a memory region.

17. (CURRENTLY AMENDED) The central processing unit according to ~~claim 3~~claim 1, wherein:

said tamper resistant buffer records unable-to-output information indicating whether or not to output corresponding information within said tamper resistant buffer to an outside of said tamper resistant buffer, and cache lock information indicating whether or not to output corresponding information to an outside of said cache; and

a move of the first license between the first program and a different program is managed based on the unable-to-output information and the cache lock information.

18. (WITHDRAWN) The central processing unit according to claim 2, wherein the first program is a trusted computing module.

19. (WITHDRAWN) The central processing unit according to claim 2, wherein the first program is a program for causing the central processing unit to implement an electronic wallet.

20. (WITHDRAWN) The central processing unit according to claim 2, wherein the first program is a program handling personal information.

21. (WITHDRAWN) The central processing unit according to claim 2, wherein the first program is a virus check program of a code installed in the central processing unit.

22. (WITHDRAWN) The central processing unit according to claim 2, wherein the first program is a mobile agent that moves among a plurality of central processing units.

23. (WITHDRAWN) The central processing unit according to claim 2, wherein:

the block which configures the first program includes hash verification requirement/nonrequirement information indicating whether or not verification of a hash value of the block is required; and

a hash unit calculating the hash value of the block, and adding the hash value to the block based on the hash verification requirement/nonrequirement information, and

a hash verifying unit verifying the hash value of the block based on the hash verification requirement/nonrequirement information are further comprised.

24. (WITHDRAWN) The central processing unit according to claim 2, wherein:

the block which configures the first program includes encryption requirement/nonrequirement information indicating whether or not the block requires protection; and

a protection block selecting unit determining whether the block is output either to said encrypting unit or to said cache or a memory region unchanged based on the encryption requirement/nonrequirement information is further comprised.

25. (WITHDRAWN) The central processing unit according to claim 2, wherein:

a header of an executable file of the first program includes an encrypted block bitmap indicating a configuration of the block which configures the first program; and

a protection block selecting unit determining whether the block is output either to said encrypting unit or to the cache or a memory region unchanged based on the encrypted block bitmap is further comprised.

26. (WITHDRAWN) The central processing unit according to claim 2, wherein:

a start of a code of the first program is a code which specifies that a plurality of blocks configuring the first program are a repetition of a combination of a plain text block and an encrypted block, and also specifies a number of successive plain text blocks, and a number of successive encrypted blocks in the combination; and

said processor core determines whether the block is output either to said encrypting unit or to said cache or a memory region unchanged by executing the code.

27. (WITHDRAWN) The central processing unit according to claim 2, further comprising between said cache and a memory

a cache line via said encrypting unit, and

a cache line not via said encrypting unit.

28. (WITHDRAWN-CURRENTLY AMENDED) A computer comprising:

a central processing unit ~~which comprises~~comprising:

an encrypting unit encrypting a block, and decrypting an encrypted block; and

a tamper resistant buffer that a user cannot reference or falsify;

wherein:

a first private key is concealed in the central processing unit in secrecy; and

said encrypting unit obtains from a first license a code decryption key for decrypting an encrypted block which configures a first program by decrypting with the first private key the first license of the first program, which is encrypted with a public key pairing with the first private key,

the code decryption key is recorded to said tamper resistant buffer,

the first license includes an access condition used when an execution process of the first program accesses a memory region, and

wherein said central processing unit further includes:

a Translation Lookaside Buffer (TLB) recording an address of the memory region, at which the encrypted block which configures the first program is recorded, and the access condition to the memory region,

a memory managing unit,

a cache, and

a processor core,

wherein said TLB and said tamper resistant buffer are linked,

wherein said memory managing unit obtains the access condition to the memory region from said TLB based on an address or a memory region, at which an encrypted block is

recorded, and further obtains the code decryption key corresponding to the memory region from said tamper resistant buffer,

wherein said processor core determines whether an access to the memory region is permitted to be made from the execution process based on the access condition obtained by said memory managing unit, and the access to the memory region is made from the execution process if said processor core determines that the access to the memory region is permitted to be made, and

wherein said encrypting unit writes to said cache a code obtained by decrypting the encrypted block within the memory region with the code decryption key obtained by said memory managing unit.

29. (WITHDRAWN) The central processing unit of claim 1, wherein said central processing unit is set in an IC card.

30. (WITHDRAWN) The central processing unit according to claim 29, wherein the first program is a program for implementing a security function of the IC card.

31. (WITHDRAWN) The central processing unit according to claim 2, which is mounted in a robot, wherein the first program is a control program for controlling the robot.

32. (WITHDRAWN) A recording device in which is recorded a program for causing a central processing unit to execute a process of a control for giving authorization to execute a protection program, wherein, the protection program to be encrypted with a code encryption key, and a license, which includes the code encryption key and is encrypted with a public key pairing with a private key comprised in secrecy within the central processing unit, is provided in correspondence with the protection program, wherein the central processing unit includes an encrypting unit encrypting a block and decrypting an encrypted block, wherein a first private key is concealed in secrecy, and said encrypting unit obtains from a first license a code decryption key for decrypting an encrypted block which configures a first program by decrypting with the first private key the first license of the first program, which is encrypted with a public key pairing with the first private key, the process comprising:

entering the license into the central processing unit before the central processing unit executes the protection program;

causing an encrypting unit comprised by the central processing unit to obtain the code

encryption key from the license by decrypting the license with the private key; and

causing the encrypting unit to decrypt the protection program with the code encryption key.

33. (WITHDRAWN) A program execution authorization method giving authorization to execute a protection program to a central processing unit, wherein, the protection code program is encrypted with a code encryption key, and a license, which includes the code encryption key and is encrypted with a public key pairing with a private key comprised within the central processing unit, is provided in correspondence with the protection program, and the central processing unit includes an encrypting unit encrypting a block and decrypting an encrypted block, wherein a first private key is concealed in secrecy, and said encrypting unit obtains from a first license a code decryption key for decrypting an encrypted block which configures a first program by decrypting with the first private key the first license of the first program, which is encrypted with a public key pairing with the first private key, said method comprising:

causing the central processing unit to obtain the license before executing the protection program;

causing the central processing unit to obtain the code encryption key from the license by decrypting the license with the private key; and

causing the central processing unit to decrypt the protection program with the code encryption key.

34. (WITHDRAWN) A computer-readable storage medium on which is recorded a program code executed by a computer, wherein:

the program code is encrypted with a code encryption key;

a license, which includes the code encryption key and is encrypted with a public key paring with a private key comprised in secrecy within a central processing unit comprised by the computer to execute the program code, is provided in correspondence with the program code;

the license is entered into the central processing unit before the program code is executed;

the license is decrypted with the private key by the central processing unit; and

the program code is decrypted with the code encryption key obtained from the license by the central processing unit.

35. (WITHDRAWN) A program generating device generating a program executed by a

central processing unit having an encrypting unit encrypting a block, and decrypting an encrypted block, wherein a first private key is concealed in secrecy, and the encrypting unit obtains from a first license a code decryption key for decrypting an encrypted block which configures a first program by decrypting with the first private key the first license of the first program, which is encrypted with a public key pairing with the first private key, said program generating device comprising:

an inputting unit inputting a code object,

a linker preprocessing unit dividing the input code object into a plurality of blocks, and adding an NOP instruction to each of the plurality of blocks,

a linker unit making an address resolution,

a protection code executable format generating unit generating a protection code executable format by encrypting each of the plurality of blocks with a code encryption key, and

a license generating unit generating a license that includes the code encryption key and is encrypted with a public key pairing with the private key, wherein:

the license is entered into the central processing unit before the computer executes the protection code executable format, and decrypted with the private key by the encrypting unit; and

the protection code executable format is decrypted with the code encryption key obtained from the license by the encrypting unit.

36. (WITHDRAWN- CURRENTLY AMENDED) A central processing unit executing a program, comprising:

encrypting means for encrypting a block, and decrypting an encrypted block; and

a tamper resistant buffer that a user cannot reference or falsify,

wherein:

a first private key is concealed in secrecy; and

said encrypting means obtains from a first license a code decryption key for decrypting an encrypted block which configures a first program by decrypting with the first private key the first license of the first program, which is encrypted with a public key pairing with the first private key,

the code decryption key is recorded to said tamper resistant buffer,

the first license includes an access condition used when an execution process of the first program accesses a memory region, and

wherein said central processing unit further includes:

a Translation Lookaside Buffer (TLB) recording an address of the memory region,

at which the encrypted block which configures the first program is recorded, and the access condition to the memory region,

a memory managing means,

a cache, and

a processor core,

wherein said TLB and said tamper resistant buffer are linked,

wherein said memory managing means obtains the access condition to the memory region from said TLB based on an address or a memory region, at which an encrypted block is recorded, and further obtains the code decryption key corresponding to the memory region from said tamper resistant buffer,

wherein said processor core determines whether an access to the memory region is permitted to be made from the execution process based on the access condition obtained by said memory managing means, and the access to the memory region is made from the execution process if said processor core determines that the access to the memory region is permitted to be made, and

wherein said encrypting means writes to said cache a code obtained by decrypting the encrypted block within the memory region with the code decryption key obtained by said memory managing means.

37. (WITHDRAWN) A program product having a program for causing a central processing unit to execute a process of a control for authorization to execute a protection program, wherein, the protection program to be encrypted with a code encryption key, and a license, which includes the code encryption key and is encrypted with a public key pairing with a private key comprised in secrecy within the central processing unit, is provided in correspondence with the protection program, and the central processing unit includes an encrypting unit encrypting a block, and decrypting an encrypted block wherein a first private key is concealed in secrecy, and said encrypting unit obtains from a first license a code decryption key for decrypting an encrypted block which configures a first program by decrypting with the first private key the first license of the first program, which is encrypted with a public key pairing with the first private key, the process comprising:

entering the license into the central processing unit before the central processing unit executes the protection program;

causing an encrypting unit comprised by the central processing unit to obtain the code encryption key from the license by decrypting the license with the private key; and

causing the encrypting unit to decrypt the protection program with the code encryption key.

38. (WITHDRAWN) A program product having a program code executed by a computer, wherein:

the program code is encrypted with a code encryption key;

a license, which includes the code encryption key and is encrypted with a public key paring with a private key comprised in secrecy within a central processing unit comprised by the computer to execute the program code, is provided in correspondence with the program code;

the license is entered into the central processing unit before the program code is executed;

the license is decrypted with the private key by the central processing unit; and

the program code is decrypted with the code encryption key obtained from the license by the central processing unit.